IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: **Blakley et al.**	§ Group Art Unit: **2157**
	§
Serial No.: **09/487,187**	§ Examiner: **Burgess, B.**
	§
Filed: **01/19/2000**	§ Atty. Docket No.: **AUS000066US1**
	§

For: **Method of Enabling An Intermediary Server to Impersonate a Client User's Identity to a Plurality of Authentication Domains**
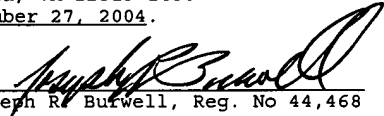
5

APPELLANT'S BRIEF
IN RESPONSE TO OFFICE ACTION UNDER 37 C.F.R. § 1.192

10   This brief is filed in triplicate in support of the previously filed Notice of Appeal, which was filed 04/27/2004, and which appealed from the decision of the examiner dated 12/22/2003 rejecting claims 1-21. The fee required under 37 C.F.R. § 1.17(c) for filing a brief in support of an appeal is

15   provided in the Transmittal of Appeal Brief filed herewith.

1. REAL PARTY IN INTEREST

The real party in interest in this appeal is International Business Machines Corporation (IBM).

2. RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

3. STATUS OF CLAIMS

Claims 1-21 are pending in this application; claims 1-21 have been finally rejected; claims 1-21 have been appealed. No claims have been canceled, withdrawn, or allowed after final.

4. STATUS OF AMENDMENTS

No after-final amendments have been filed.

5. SUMMARY OF INVENTION

An enterprise computing environment, such as a corporate web portal, includes an intermediary server (Specification, page 9, line 1; Figure 2), a sign-on service (Page 9, line 2; Figure 2, and one or more backend enterprise systems managed by resource managers (Page 9, line 3; Figure 2). Before or after user primary logon, which establishes a user primary account identity, the intermediary server uses its own identity to authenticate to the sign-on service its right to retrieve user secondary account identities with respect to the backend enterprise systems (Page 12, line 16). Retrieved secondary account identities are then used by the intermediary server to perform user secondary logons to respective resource managers in the environment (Page 13, lines 5; step 306, Figure 3). The intermediary server also manages the passing of resource requests and associated replies between the user and the resource managers.

6. ISSUES

The issues on appeal are:

(A) whether claims 1-6, 8-14, 16, 17, and 19-21 are anticipated under 35 U.S.C. § 102(b) by Hu, "Method and apparatus for authenticating a client to a server in computer systems which support different security mechanisms", U.S. Patent No. 5,586,260, issued 12/17/1996; and

(B) whether claims 7, 15, and 18 are unpatentable under 35 U.S.C. § 103(a) over Hu in view of Brendel et al., "World-Wide-Web Server with Delayed Resource-Binding for Resource-Based Load Balancing on A Distributed Resource Multi-Node Network, issued 06/30/1998.

7. GROUPING OF CLAIMS

The entire set of claims do not stand or fall together but are grouped as follows:

(A) Claims 1-6, 8-14, 16, 17, and 19-21 stand or fall together;

(B) Claims 7, 15, and 18 stand or fall together.

8. ARGUMENTS

8.A.

Was 35 U.S.C. § 102(b) properly applied in a rejection of claims 1-6, 8-14, 16, 17, and 19-21 as being anticipated by Hu?

Independent claims 1, 10, and 11 are directed to a method, whereas independent claims 12, 14, and 16 are directed to a corresponding system or server, and independent claim 21 is directed to a corresponding computer program product. Since claim 1 is broader than the other claims, claim 1 is used herein as an exemplary claim.

All of the pending independent claims have been rejected over Hu. Each of these independent claims has one or more common elements against which the rejection applies certain portions of Hu. However, Appellant asserts that there is at least one element of each independent claim that is not shown in Hu, thereby causing these anticipation rejections to be deficient. However, prior to discussing these rejections in more detail, Appellant makes the following preliminary comparison of Hu and the present invention.

The abstract of <u>Hu</u> states in its entirety:

> A method and corresponding apparatus for authenticating a client for a server when the client and server have different security mechanisms. An intermediary system known as an authentication gateway provides for authentication of the client using the client security mechanism, and impersonation of the client in a call to a server that the client wishes to access. The client logs in to the authentication gateway and provides a user name and password. Then the authentication gateway obtains and saves security credentials for the client, returning an access key to the client. When the client wishes to call the server, the client calls the authentication gateway acting as a proxy server, and passes the access key, which is then used to retrieve the security credentials and to impersonate the client in a call to the server. Any output arguments resulting from the call to the server are returned to the client through the authentication gateway.

These steps are shown within **FIG. 2** and **FIG. 3** of <u>Hu</u>.

<u>Hu</u> explains its Figure 2 and Figure 3 at lines 5 through 58 in column 4 as follows:

> **FIG. 2** shows the gateway computer system **14** as including a proxy server process **20** and an authentication gateway process **22**. As will be further explained, the authentication gateway process **22** authenticates the client within the client security domain **18**. When the client system **10** makes a request to use the server **12**, the request is processed by the proxy server **20**, which obtains the client credentials from the gateway authentication process **22**, and then makes a call to the real server **12**, effectively impersonating the client **10**. If the service requested of the server **12** requires that information be passed back to the client from the server, this information is passed through the proxy server **20** acting as an intermediary.
>
> **FIG. 3** takes the explanation of the authentication gateway scheme one step further, and shows diagrammatically the sequence of steps followed by each of the systems in handling access to the server **12** by a client system **10** not conforming with the security mechanism of the server. The client system **10** includes a log-in procedure **30**, and a client application process **32** from which a server request will emanate. The log-in procedure **30** is executed, as its name implies, only infrequently, such as once a day. Part of the log-in procedure is a call to the authentication gateway **22** to permit authentication within the client security domain. This call, indicated by line **34** carries as parameters the identity of the client and any necessary password or security code needed to satisfy the security requirements of the client security domain. The authentication gateway **22** performs the operations necessary to

verify the authenticity of the client **10**. The authentication
gateway **22** acquires authentication credentials for the client and
saves them for later use. The authentication gateway **22** then
returns to the log-in procedure **30**, over line **36**, an identifier
that confirms authentication of the client. The log-in procedure
30 stores the returned identifier in an id. cache **38**. This
completes the first phase of operation of the gateway, which has
authenticated the client within the client's security domain and
has stored a confirming identifier in the cache **38**, over line **40**
for later use by the client.

Subsequently, when the client application process **32** wishes
to make a call to the server, the contents of the id. cache are
retrieved, as indicated by the broken line **42**, and the client
makes a call to the proxy server process **20**, as indicated by line
42, passing as an argument of the call the identifier obtained
from the cache **38**. Then, using the identifier, the proxy server
20 calls the authentication gateway **22**, as indicated by line **44**,
and acquires, over line **46**, the credentials of the client that
were saved by the authentication gateway during the log-in
procedure. At this point the proxy server has all the information
it needs to make a call to the real server **12**, as indicated by
line **48**. Information generated as a result of the call to the
server **12** is passed back to the client application process **32**,
through lines **48** and **43**.

As stated in column 5, lines 63-65: "The log-in procedure
prompts the user for a user name and a password based on the
server security domain." Thus, in the system disclosed in Hu, a
user has one user identity for each security domain that the user
accesses. The credentials that result from the login procedure
are cached by the authentication gateway process **22** for later use
by the proxy server process **20**; these two entities subsequently
interact when the proxy server process calls the authentication
gateway process to retrieve the previously cached credential for
a particular security domain. Hence, the system of Hu is useful
because a user performs multiple login procedures for the
multiple server security domains that are accessed, and the
cached credentials may be re-used without the user having to
perform the login procedure again.

However, the system of Hu does not disclose a plurality of
user identities that are derived from a single user identity and

then used by a single-sign-on service, such as a primary user
identity and a set of secondary user identities as disclosed and
claimed in the present patent application. As explained in more
detail further below, Appellant asserts that the rejection has
misinterpreted the manner in which the system of Hu employs
multiple user identities and improperly states that Hu discloses
the employment of multiple user identities as taught by the
present invention.

With reference now to independent claim 1, Appellant asserts
that Hu does not disclose all of the elements of claim 1. The
rejection states in its entirety:

> As per claim 1, Hu discloses a method of enabling a
> client terminal user to access target resources managed by a
> set of resource managers within an enterprise computing
> environment, comprising:
> authenticating the user to establish a user primary
> identity (column 1, lines 52-55, column 2, lines 3-5, 30-35,
> 42-45, column 4, lines 23-28);
> mapping the user primary identity to a set of user
> secondary identities (column 2, lines 1-17, 20-25, 42-47,
> column 4, lines 44-55, column 5, lines 30-35, 60-67, column
> 6, lines 1-11, 17-30);
> authenticating the user to the resource managers using
> the set of secondary identities (column 2, lines 1-17,
> 20-25, 42-47, column 4, lines 44-55, column 5, lines 30-35,
> 60-67, column 6, lines 1-11, 17-30);
> following authentication using the set of user
> secondary identities, forwarding resource requests to the
> resource managers (column 3, lines 63-65, column 4, lines
> 53-55, column 6, lines 31-35);
> returning replies received from the resource managers
> back to the user (column 4, lines 14-17, 55-58, column 6,
> lines 35-39).

As should be apparent from a cursory reading of the
rejection, the rejection has taken multiple shortcuts in terms of
form and logic that make it difficult for one to understand the
anticipation argument that is supposedly presented by the

rejection. For example, it is difficult to understand why the same portions of Hu are cited as disclosing different elements within the claim. Additionally, it is difficult to understand why multiple portions of Hu are cited for disclosing one element within the claim. Moreover, some of the cited portions of Hu contain many different kinds of processing steps, and it is difficult to understand why the anticipation rejection does not attempt to relate individual steps within Hu to the individual steps in the method of claim 1. Thus, Appellant must attempt to construct a logical argument from the cited portions without any additional statements within the rejection.

Appellant asserts that Hu does not disclose "a user primary identity" nor "a set of user secondary identities". Hence, it is not possible for Hu to disclose the second element of claim 1, "mapping the user primary identity to a set of user secondary identities".

Even though Hu does not disclose a user primary identity, one could argue that it does disclose a user identity, and then one could proceed to consider this user identity as a user primary identity. From that point, one could argue that the first element of claim 1, "authenticating the user to establish a user primary identity", is disclosed by the login procedure 30 that is shown in Figure 3 of Hu. As noted above, the user provides a user name (user identity) during the login procedure based on the security domain. This authentication procedure results in a single cached identifier that relates to the cached credentials for a security domain. This cached identifier is subsequently provided to the proxy server 20, which then provides the identifier to the authentication gateway 22.

The authentication gateway then uses the identifier to retrieve the credentials that were previously saved by the

authentication gateway during a login procedure; the identifier associates the credentials for a security domain with the user identity that was provided during the login procedure. In this manner, the authentication gateway maps a single user identity to the credentials for the security domain that was used in the login procedure. However, Hu does not disclose "mapping the user primary identity to a set of user secondary identities", as claimed in claim 1.

Taking a different approach, one could argue that Hu does disclose a set of user identities, each of which is associated with a security domain; the user must provide a user name and a password for each security domain into which the user performs a login procedure. One could proceed to argue that these user identities are a set of user secondary identities. From that point, one could argue that the third element of claim 1, "authenticating the user to the resource managers using the set of user secondary identities", is disclosed by multiple repetitions of the login procedure 30 that is shown in Figure 3 of Hu. However, one would not be able to argue that Hu discloses a user primary identity nor, more importantly, "authenticating the user to establish a user primary identity", as stated in the first element of claim 1. Each of the user identities in Hu should be considered as having similar characteristics, and no user identity is distinguished as being a user primary identity. Moreover, Hu still does not disclose "mapping the user primary identity to a set of user secondary identities", as stated in the second element of claim 1.

Hence, Hu does not disclose at least one element of claim 1 as is required for a proper anticipation rejection. As stated at MPEP § 2131: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or

inherently described, in a single prior art reference."
Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628,
631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical
invention must be shown in as complete detail as is contained in
5   the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226,
1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Hence, the rejection
of claim 1 is improper, and Appellant requests that the rejection
should not be upheld on appeal.

10   <u>8.B.</u>

**Was 35 U.S.C. § 103(a) properly applied in a rejection of
claims 7, 15, and 18 as being unpatentable over <u>Hu</u> in view of
<u>Brendel et al.</u>?**

15   Claim 7 is directed to a method, whereas claims 15 and 18
are directed to a corresponding system or server. Since claim 7
is broader than the other claims, claim 7 is used herein as an
exemplary claim.

With respect to dependent claim 7, the rejection properly
20   states that <u>Brendel et al.</u> discloses a load-balancing mechanism
as recited in claim 7. However, claim 7 depends from claim 1,
and as argued above, <u>Hu</u> fails to disclose the features of these
independent claims. Moreover, <u>Brendel et al.</u> also fails to
disclose the features of these independent claims. Hence, a
25   combination of the teaching of <u>Brendel et al.</u> with <u>Hu</u> cannot
support a rejection of dependent claim 7 because at least one
feature of the independent claims has not been disclosed in the
prior art. Appellant respectfully submits that more than one
claimed feature is not shown in the prior art references nor can
30   the teachings of the references be combined to disclose the
present invention. Hence, the rejection of claim 7 does not

establish a *prima facie* case of obviousness based on the prior art. Therefore, the rejection of claim 7 under 35 U.S.C. § 103(a) has been shown to be insupportable, and these claims are patentable over the applied references. Appellant requests that

5   the rejection should not be upheld on appeal.

9. Conclusion

In view of the above arguments, it is respectfully urged that the rejection of the claims should not be sustained.

10

DATE: September 27, 2004   Respectfully submitted,

Joseph R. Burwell
15   Reg. No. 44,468
ATTORNEY FOR APPELLANT

Law Office of Joseph R. Burwell
P.O. Box 28022
20   Austin, Texas 78755-8022
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz

10. APPENDIX OF CLAIMS

1. A method of enabling a client terminal user to access target resources managed by a set of resource managers within an enterprise computing environment, comprising:

authenticating the user to establish a user primary identity;

mapping the user primary identity to a set of user secondary identities;

authenticating the user to the resource managers using the set of user secondary identities;

following authentication using the set of user secondary identities, forwarding resource requests to the resource managers; and

returning replies received from the resource managers back to the user.

2. The method as described in claim 1 wherein the user primary identity is mapped to the set of user secondary identities by a sign-on service.

3. The method as described in claim 2 further including the step of authenticating a trusted server to the sign-on service prior to mapping the user primary identity to the set of user secondary identities.

4. The method as described in claim 3 wherein the trusted server is authenticated to the sign-on server before the step of authenticating the user to establish the user primary identity.

5.   The method as described in claim 3 wherein the trusted
server is authenticated to the sign-on service after the step of
authenticating the user to establish the user primary identity.

5   6.   The method as described in claim 3 wherein the user is
authenticated to establish the user primary identity using an
authentication service associated with the trusted server.

7.   The method as described in claim 1 further including the
10   step of load balancing resource requests across a set of
instances of a given resource manager.

8.   The method as described in claim 1 wherein the client
terminal user accesses the enterprise computing environment over
15   the Internet.

9.   The method as described in claim 1 wherein the user is
authenticated to a given resource manager using an authentication
service associated with the given resource manager.

20

10. A method for enabling a client terminal user to access target resources managed by a set of resource managers operative within an enterprise computing environment, wherein the environment has an associated sign-on service, comprising:

responsive to a request received from a user of the client terminal, authenticating the user to establish a user primary identity;

using the user primary identity, accessing the sign-on service to retrieve a set of stored user authentication information, wherein the stored user authentication information comprises a set of user secondary identities;

performing a sign-on to the set of resource managers using the retrieved set of user secondary identities; and

forwarding the request to a given resource manager; and

forwarding a reply received from the given resource manager back to the user.

11. A method for enabling a client terminal user to access target resources managed by a set of resource managers operative within an enterprise computing environment, wherein the environment has an associated sign-on service, comprising:

5   having the client terminal user perform a primary logon to an intermediary server to establish a user primary identity;

having the intermediary server pass the user's primary identity to the sign-on service and, in response, obtaining a set of user secondary identities that may be used in enabling the

10   intermediary server to represent the client terminal user to the resource managers;

having the intermediary server perform a secondary logon to a first resource manager using a first user secondary identity;

having the intermediary server perform a secondary logon to

15   a second resource manager using a second user secondary identity;

having the intermediary server perform resource requests at the first and second resource managers under the respective secondary identities; and

forwarding responses back to the client terminal user.

20

12. An enterprise computing environment having a set of resource managers and a sign-on service, the enterprise computing environment comprising:

   means for authenticating a user to establish a user primary
5 account associated with a user primary identity;

   means for cooperating with the sign-on service to map the user primary account to a set of user secondary accounts associated with a set of user secondary identities;

   means for logging onto the set of resource managers using
10 the user secondary accounts; and

   means for passing resource requests from the user to the resource managers under the user secondary accounts.

13. The enterprise computing environment as described in claim
15 12 wherein the server passes replies to the resource requests back to the user.

14. A server for use in an enterprise computing environment having a set of resource managers and a sign-on service, comprising:

means for authenticating a user to establish a user primary
5   account associated with a user primary identity;

means for authenticating the server to the sign-on service;

means for logging onto the set of resource managers using a set of user secondary accounts returned from the sign-on service, wherein the set of user secondary accounts is associated with a
10   set of user secondary identities; and

means for passing resource requests and associated replies between the user and the resource managers.

15. The server as described in claim 14 further including means
15   for load balancing resource requests passed to a set of instances of a given resource manager.

16. A system, comprising:

a set of resource managers;

a sign on service;

a server, comprising:

means for authenticating users to establish user primary accounts associated with user primary identities;

means for logging a given user onto the set of resource managers using a set of user secondary accounts for the given user retrieved from the sign on service, wherein a set of user secondary accounts for a given user is associated with a set of user secondary identities for a given user; and

means for passing resource requests and associated replies between the given user and the resource managers.

17. The system as described in claim 16 wherein at least one resource manager comprises a set of instances.

18. The system as described in claim 17 wherein the server further includes means for load balancing resource requests across the set of instances.

19. The system as described in claim 16 wherein the server comprises a set of instances.

20. The system as described in claim 19 further including a manager that manages the set of server instances.

21. A computer program product in a computer-useable medium executable in a processor of a server, comprising:

means for authenticating a user to establish a user primary account associated with a user primary identity;

5   means for authenticating the server to a sign-on service;

means for logging onto a set of resource managers using a set of user secondary accounts returned from the sign-on service, wherein the set of user secondary accounts are associated with a set of user secondary identities; and

10   means for passing resource requests and associated replies between the user and the resource managers.